

1 Делимость. Системы счисления. Алгоритм Евклида.

1.1 Признаки делимости

Натуральное число делится на 2 тогда и только тогда, когда его последняя цифра делится на 2, то есть является чётной.

Натуральное число делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

Натуральное число делится на 4 тогда и только тогда, когда две его последние цифры составляют число, которое делится на 4. Двухзначное число делится на 4 тогда и только тогда, когда удвоенное число десятков, сложенное с числом единиц делится на 4.

Натуральное число делится на 5 тогда и только тогда, когда последняя цифра делится на 5, т.е. если она 0 или 5.

Натуральное число делится на 6 тогда и только тогда, когда оно делится и на 2, и на 3, то есть если оно четное и сумма его цифр делится на 3.

Натуральное число делится на 7 тогда и только тогда, когда разность между этим числом без его последней цифры и удвоенной последней цифрой делится на 7.

Натуральное число делится на 8 тогда и только тогда, когда три его последние цифры составляют число, которое делится на 8.

Натуральное число делится на 9 тогда и только тогда, когда сумма его цифр делится на 9.

Натуральное число делится на 10 тогда и только тогда, когда оно оканчивается на ноль.

Натуральное число делится на 11 тогда и только тогда, когда сумма цифр стоящих на четных местах равна сумме цифр стоящих на нечетных местах или отличается от нее на число, кратное 11.

1.2 Системы счисления

Существуют позиционные и непозиционные системы счисления. Арабская система счисления, которым мы пользуемся в повседневной жизни, является позиционной, а римская — нет. В позиционных системах счисления позиция числа однозначно определяет величину числа.

Пример 1. Возьмём число 5921 в десятичной системе счисления. Пронумеруем его разряды справа налево начиная с нуля:

Число	5	9	2	1
Номер разряда	3	2	1	0

Число 5921_{10} можно записать в следующем виде:

$$5921_{10} = 5000 + 900 + 20 + 1 = 5 \cdot 10^3 + 9 \cdot 10^2 + 2 \cdot 10^1 + 1 \cdot 10^0.$$

Число 10 является характеристикой, определяющей систему счисления. В качестве показателей степеней взяты номера соответствующих разрядов числа.

Пример 2. Рассмотрим вещественное десятичное число 1234,567. Пронумеруем его разряды, начиная с нулевого от запятой влево и вправо:

Число	1	2	3	4	5	6	7
Номер разряда	3	2	1	0	-1	-2	-3

Число 1234,567 можно записать в следующем виде:

$$1234,567_{10} = 1000 + 200 + 30 + 4 + 0.5 + 0.06 + 0.007 =$$

$$= 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0 + 5 \cdot 10^{-1} + 6 \cdot 10^{-2} + 7 \cdot 10^{-3}.$$

В общем случае формулу можно представить в следующем виде:

$$I_n \cdot s^n + I_{n-1} \cdot s^{n-1} + \dots + I_1 \cdot s^1 + I_0 \cdot s^0 + F_{-1} \cdot s^{-1} + F_{-2} \cdot s^{-2} + \dots + F_{-k} \cdot s^{-k}. \quad (1)$$

где I_n — целое число в позиции n , F_{-k} — дробное число в позиции $(-k)$, s — система счисления.

Несколько слов о системах счисления. Число в десятичной системе счисления состоит из множества цифр $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, в восьмеричной системе счисления — из множества цифр $\{0, 1, 2, 3, 4, 5, 6, 7\}$, в двоичной системе счисления — из множества цифр $\{0, 1\}$, в шестнадцатеричной системе счисления — из множества цифр $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$, где A, B, C, D, E, F являются цифрами и соответствуют числам 10, 11, 12, 13, 14, 15.

В таблице представлены числа в разных системах счисления.

Система счисления			
10	2	8	16
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F

1.3 Перевод чисел из одной системы счисления в другую

Наиболее простым способом перевода числа из одной системы счисления в другую, является перевод числа сначала в десятичную систему счисления с последующим переводом полученного результата в требуемую систему счисления.

1.3.1 Перевод чисел из любой системы счисления в десятичную систему счисления

Для перевода числа из любой системы счисления в десятичную достаточно пронумеровать его разряды, начиная с нулевого (разряд слева от десятичной точки) аналогично примерам 1 или 2. Найдём сумму произведений цифр числа на основание системы счисления в степени позиции этой цифры:

Пример 3. Перевести число 1001101.1101_2 в десятичную систему счисления.

Решение:

$$\begin{aligned} 10011.1101_2 &= 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 + 1 \cdot 2^{-1} + 1 \cdot 2^{-2} + 0 \cdot 2^{-3} + 1 \cdot 2^{-4} = \\ &= 16 + 2 + 1 + 0.5 + 0.25 + 0.0625 = 19.8125_{10} \end{aligned}$$

Ответ: $10011.1101_2 = 19.8125_{10}$.

Пример 4. Перевести число $E8F.2D_{16}$ в десятичную систему счисления.

Решение:

$$\begin{aligned} E8F.2D_{16} &= 14 \cdot 16^2 + 8 \cdot 16^1 + 15 \cdot 16^0 + 2 \cdot 16^{-1} + 13 \cdot 16^{-2} = \\ &= 3584 + 128 + 15 + 0.125 + 0.05078125 = 3727.17578125_{10} \end{aligned}$$

Ответ: $E8F.2D_{16} = 3727.17578125_{10}$.

1.3.2 Перевод чисел из десятичной системы счисления в другую систему счисления

Для перевода чисел из десятичной системы счисления в другую систему счисления целую и дробную части числа нужно переводить отдельно.

1.3.3 Перевод целой части числа из десятичной системы счисления в другую систему счисления

Целая часть переводится из десятичной системы счисления в другую систему счисления с помощью последовательного деления целой части числа на основание системы счисления до получения целого остатка, меньшего основания системы счисления. Результатом перевода будет являться запись из остатков, начиная с последнего.

Пример 5. Перевести число 273_{10} в восьмиричную систему счисления.

Решение: $273/8 = 34$ и остаток 1, $34/8 = 4$ и остаток 2, 4 меньше 8, поэтому вычисления завершены. Запись из остатков будет иметь следующий вид: 421_8 .

Проверка: $4 \cdot 8^2 + 2 \cdot 8^1 + 1 \cdot 8^0 = 256 + 16 + 1 = 273 = 273$, результат совпал. Значит перевод выполнен правильно.

Ответ: $273_{10} = 421_8$.

Пример 6. Переведем число 159 из десятичной СС в двоичную СС:

Решение:	159	2	79	1
	79	2	39	1
	39	2	19	1
	19	2	9	1
	9	2	4	1
	4	2	2	0
	2	2	1	0
	1	2	0	1

Как видно, число 159 при делении на 2 дает частное 79 и остаток 1. Далее число 79 при делении на 2 дает частное 39 и остаток 1 и т.д. В результате построив число из остатков деления (справа налево) получим число в двоичной СС: 10011111. Следовательно можно записать:

Ответ: $159_{10} = 10011111_2$.

Пример 7. Переведем число 615 из десятичной СС в восьмеричную СС.

Решение:	615	8	76	7
	76	8	9	4
	9	8	1	1
	1	8	0	1

При приведении числа из десятичной СС в восьмеричную СС, нужно последовательно делить число на 8, пока не получится целый остаток меньше, чем 8. В результате построив число из остатков деления (справа налево) получим число в восьмеричной СС: 1147. Следовательно можно записать:

Ответ: $615_{10} = 1147_8$.

Пример 8. Переведем число 19673 из десятичной системы счисления в шестнадцатеричную СС.

Решение:	19673	16	1229	9
	1229	16	76	13
	76	16	4	12
	4	16	0	4

Как видно выше, последовательным делением числа 19673 на 16 получили остатки 4, 12, 13, 9. В шестнадцатеричной системе счисления числу 12 соответствует цифра C , числу 13 — цифра D . Следовательно наше шестнадцатеричное число — это $4CD9$.

Ответ: $19673_{10} = 4CD9_{16}$.

Рассмотрим перевод правильных десятичных дробей в различные системы счисления.

1.3.4 Перевод дробной части числа из десятичной системы счисления в другую систему счисления

Напомним, что правильной десятичной дробью называется вещественное число с нулевой целой частью. Чтобы перевести такое число в систему счисления с основанием N нужно последовательно умножать число на N до тех пор, пока дробная часть не обнулится или же не будет получено требуемое количество разрядов. Если при умножении получается число с целой частью, отличное от нуля, то целая часть дальше не учитывается. При этом целая часть последовательно заносится в результат.

Пример 9. Перевести число 0.125_{10} в двоичную систему счисления.

Решение: $0.125 \cdot 2 = 0.25$ (0 — целая часть, которая станет первой цифрой результата), $0.25 \cdot 2 = 0.5$ (0 — вторая цифра результата), $0.5 \cdot 2 = 1.0$ (1 — третья цифра результата, а так как дробная часть равна нулю, то перевод завершён).

Ответ: $0.125_{10} = 0.001_2$.

Пример 10. Переведем число 0,214 из десятичной системы счисления в двоичную СС до 7 знака после запятой.

							0,214
			×				2
		0					0,428
			×				2
		0					0,856
			×				2
		1					0,712
Решение:			×				2
		1					0,424
			×				2
		0					0,848
			×				2
		1					0,696
			×				2
		1					0,392

Как видно, число 0,214 последовательно умножается на 2. Если в результате умножения получится число с целой частью, отличное от нуля, то целая часть записывается отдельно (слева от числа), а число записывается с нулевой целой частью. Если же при умножении получится число с нулевой целой частью, то слева от нее записывается нуль. Процесс умножения продолжается до тех пор, пока в дробной части не получится чистый нуль или же не получим требуемое количество разрядов. Записывая жирные числа сверху вниз получим требуемое число в двоичной системе счисления: 0,0011011.

Ответ: $0,214_{10} = 0,0011011_2 (\pm 0,0000001_2)$.

Пример 11. Переведем число 0.125 из десятичной системы счисления в двоичную СС.

							0.125
			×				2
		0					0.25
Решение:			×				2
		0					0.5
			×				2
		1					0.0

Для приведения числа 0.125 из десятичной СС в двоичную, данное число последовательно умножается на 2. На третьем этапе получилось 0.

Ответ: $0.125_{10} = 0.001_2$.

Пример 12. Переведем число 0,214 из десятичной системы счисления в шестнадцатеричную СС до 6 знака после запятой.

$$\begin{array}{r}
214 \\
\times 16 \\
\hline
\mathbf{3} 424 \\
\times 16 \\
\hline
\mathbf{6} 784 \\
\times 16 \\
\hline
\mathbf{Решение: 12} 544 \\
\times 16 \\
\hline
\mathbf{8} 704 \\
\times 16 \\
\hline
\mathbf{11} 264 \\
\times 16 \\
\hline
\mathbf{4} 224
\end{array}$$

Следуя примерам 4 и 5 получаем числа 3, 6, 12, 8, 11, 4. Но в шестнадцатеричной СС числам 12 и 11 соответствуют цифры C и B .

Ответ: $0,214_{10} = 0.36C8B4_{16} (\pm 0,000001_{16})$.

Пример 13. Переведем число 0,512 из десятичной системы счисления в восьмеричную СС до 6 знака после запятой.

$$\begin{array}{r}
512 \\
\times 8 \\
\hline
\mathbf{4} 096 \\
\times 8 \\
\hline
\mathbf{0} 768 \\
\times 8 \\
\hline
\mathbf{Решение: 6} 144 \\
\times 8 \\
\hline
\mathbf{1} 152 \\
\times 8 \\
\hline
\mathbf{1} 216 \\
\times 8 \\
\hline
\mathbf{1} 728
\end{array}$$

Ответ: $0.512_{10} = 0.406111_8 (\pm 0,000001_8)$.

Пример 14. Переведем число 159.125 из десятичной системы счисления в двоичную СС. Для этого переведем отдельно целую часть числа (Пример 4) и дробную часть числа (Пример 8). Далее объединяя эти результаты получим:

Ответ: $159.125_{10} = 10011111.001_2$.

Пример 15. Переведем число 19673.214 из десятичной системы счисления в шестнадцатеричную СС до шестого знака после запятой. Для этого переведем отдельно целую часть числа (Пример 6) и дробную часть числа (Пример 9). Далее объединяя эти результаты получим:

Ответ: $19673.214_{10} = 4CD9.36C8B4_{16} (\pm 0,000001_{16})$.

1.4 Алгоритм Евклида для целых чисел

Пусть a и b — целые числа, не равные одновременно нулю, и последовательность чисел

$$a > b > r_1 > r_2 > r_3 > r_4 > \dots > r_n$$

определена тем, что каждое r_k — это остаток от деления предпредыдущего числа на предыдущее, а предпоследнее делится на последнее нацело, то есть:

$$\begin{aligned} a &= bq_0 + r_1, \\ b &= r_1q_1 + r_2, \\ r_1 &= r_2q_2 + r_3, \\ &\dots \\ r_{k-2} &= r_{k-1}q_{k-1} + r_k, \\ &\dots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \\ r_{n-1} &= r_nq_n. \end{aligned}$$

Тогда $\text{НОД}(a, b)$, наибольший общий делитель a и b , равен r_n , последнему ненулевому члену этой последовательности.

Существование таких r_1, r_2, \dots, r_n , то есть возможность деления числа m на число n с остатком для любого целого m и целого $n \neq 0$, доказывается индукцией по m .

Корректность этого алгоритма вытекает из следующих двух утверждений:

Пусть $a = b \cdot q + r$, тогда $\text{НОД}(a, b) = \text{НОД}(b, r)$.

Доказательство Пусть k — любой общий делитель чисел a и b , не обязательно наибольший, тогда $a = t_1 \cdot k$ и $b = t_2 \cdot k$, где t_1 и t_2 — целые числа из определения. Тогда k является также общим делителем чисел b и r , так как b делится на k по определению, а $r = a - b \cdot q = (t_1 - t_2 \cdot q) \cdot k$ (выражение в скобках есть целое число, следовательно, k делит r без остатка).

Обратное также верно и доказывается аналогично пункту 2: любой делитель b и r так же является делителем a и b . Следовательно, все общие делители пар чисел (a, b) и (b, r) совпадают. Другими словами, нет общего делителя у чисел (a, b) , который не был бы также делителем (b, r) , и наоборот. В частности, наибольший общий делитель остается тем же самым. Что и требовалось доказать.

$\text{НОД}(r, 0) = r$ для любого ненулевого r (так как 0 делится на любое целое число, кроме нуля).

1.4.1 Расширенный алгоритм Евклида и соотношение Безу

Формулы для r_i могут быть переписаны следующим образом:

$$\begin{aligned} r_1 &= a + b(-q_0) \\ r_2 &= b - r_1q_1 = a(-q_1) + b(1 + q_1q_0) \\ &\dots \\ \text{НОД}(a, b) &= r_n = as + bt \end{aligned}$$

Здесь s и t целые. Это представление наибольшего общего делителя называется соотношением Безу, а числа s и t — коэффициентами Безу. Соотношение Безу является ключевым в доказательстве леммы Евклида и основной теоремы арифметики.

1.4.2 Алгоритм Евклида для многочленов

Алгоритм Евклида позволяет найти наибольший общий делитель двух многочленов, т.е. многочлен наибольшей степени, на который делятся без остатка оба данных многочлена. Алгоритм основан на том факте, что для любых двух многочленов от одного переменного, $f(x)$ и $g(x)$, существуют такие многочлены $q(x)$ и $r(x)$, называемые соответственно частное и остаток, что $f(x) = g(x) \cdot q(x) + r(x)$, при этом степень остатка меньше степени делителя, многочлена $g(x)$, и, кроме того, по данным многочленам $f(x)$ и $g(x)$ частное и остаток находятся однозначно. Если в последнем равенстве остаток $r(x)$ равен нулевому многочлену (нулю), то говорят, что многочлен $f(x)$ делится на $g(x)$ без остатка. Алгоритм состоит из последовательного деления с остатком сначала первого данного многочлена, $f(x)$, на второй, $g(x)$:

$$f(x) = g(x) \cdot q_1(x) + r_1(x) \quad (2)$$

затем, если $r_1(x) \neq 0$, — второго данного многочлена, $g(x)$, на первый остаток — на многочлен $r_1(x)$:

$$g(x) = r_1(x) \cdot q_2(x) + r_2(x), \quad (3)$$

далее, если $r_2(x) \neq 0$, — первого остатка, $r_1(x)$, на второй остаток, $r_2(x)$:

$$r_1(x) = r_2(x) \cdot q_3(x) + r_3(x), \quad (4)$$

затем, если $r_3(x) \neq 0$, — второго остатка на третий:

$$r_2(x) = r_3(x) \cdot q_4(x) + r_4(x), \quad (5)$$

и т.д. Поскольку на каждом этапе степень очередного остатка уменьшается, процесс не может продолжаться бесконечно, так что на некотором этапе мы обязательно придем к ситуации, когда очередной, $n + 1$ -й остаток r_{n+1} равен нулю:

$$r_{n+2}(x) = r_{n+1}(x) \cdot q_n(x) + r_n(x), \quad (6)$$

$$r_{n+1}(x) = r_n(x) \cdot q_{n+1}(x) + r_{n+1}(x), \quad (7)$$

$$r_{n+1}(x) = 0. \quad (8)$$

Тогда последний не равный нулю остаток r_n и будет наибольшим общим делителем исходной пары многочленов $f(x)$ и $g(x)$. Действительно, если в силу равенства 8 подставить 0 вместо $r_{n+1}(x)$ в равенство 7, затем, полученное равенство $r_{n+1}(x) = r_n(x) \cdot q_{n+1}(x)$ вместо $r_{n+1}(x)$ — в равенство 6, получится, что $r_{n+2}(x) = r_n(x) \cdot q_n + 1(x)q_n(x) + r_n(x)$, т.е. $r_{n+2}(x) = r_n(x)(q_{n+1}(x)q_n(x) + 1)$, и т.д. В равенстве 3 после подстановки получим, что $g(x) = r_n(x) \cdot Q(x)$, и, наконец, из равенства 2 — что $f(x) = r_n(x) \cdot S(x)$, где Q и S — некоторые многочлены. Таким образом, $r_n(x)$ — общий делитель двух исходных многочленов, а то, что он наибольший (т.е. наибольшей возможной степени), следует из процедуры алгоритма. Если наибольший общий делитель двух многочленов не содержит переменную (т.е. является числом), исходные многочлены $f(x)$ и $g(x)$ называются взаимно-простыми.

Пример 16. Рассмотрим многочлены $x^5 - x^4 + x^3 - x^2 + x - 1$ и $x^5 + x^3 + x^2 + 1$.

I. Найдём их НОД.

1. Поскольку степени многочленов равны, то первым действием надо вычесть один из другого (в любом порядке): $x^5 + x^3 + x^2 + 1 - (x^5 - x^4 + x^3 - x^2 + x - 1) = x^4 + 2x^2 - x + 2$.

2. Теперь делим один из многочленов большей степени на их разность (пока ещё всё равно какой)

$$\begin{array}{r|l} x^5 - x^4 + x^3 - x^2 + x - 1 & x^4 + 2x^2 - x + 2 \\ x^5 & + 2x^3 - x^2 + 2x & \hline -x^4 - x^3 & -x - 1 \\ -x^4 & -2x^2 + x - 2 \\ \hline & -x^3 + 2x^2 - 2x + 1 \end{array}$$

Отметим что $x^5 - x^4 + x^3 - x^2 + x - 1 = (x^4 + 2x^2 - x + 2)(x - 1) - x^3 + 2x^2 - 2x + 1$. (Для нахождения НОДа это выражение не нужно.)

3. Делим делитель предыдущего действия на остаток (тоже предыдущего действия). Для удобства умножим $-x^3 + 2x^2 - 2x + 1$ на -1 .

$$\begin{array}{r|l} x^4 & + 2x^2 - x + 2 & \hline x^4 - 2x^3 + 2x^2 - x & + 2 & \hline & 2x^3 & \\ & 2x^3 - 4x^2 + 4x - 2 & \\ \hline & 4x^2 - 4x + 4 & \end{array}$$

Отметим что $x^4 + 2x^2 - x + 2 = (x^3 - 2x^2 + 2x - 2)(x + 2) + 4(x^2 - x + 1)$.

4. Делим делитель предыдущего действия на остаток (тоже предыдущего действия). Для удобства умножим $4(x^2 - x + 1)$ на $\frac{-1}{4}$.

$$\begin{array}{r|l} x^3 - 2x^2 + 2x - 1 & x^2 - x + 1 \\ x^3 - x^2 + x & \hline -x^2 + x - 1 & \\ -x^2 + x - 1 & \\ \hline & 0 \end{array}$$

На этом шаге получается деление без остатка. Следовательно, многочлен $x^2 - x + 1$ является наибольшим общим делителем исходных многочленов.

II. Найдём такие многочлены $P(x)$ и $Q(x)$, что $P(x) \times (x^5 - x^4 + x^3 - x^2 + x - 1) + Q(x) \times (x^5 + x^3 + x^2 + 1) = 4(x^2 - x + 1)$.

Используя промежуточные результаты, полученные при нахождении НОД, получаем:

$$\begin{aligned} 4(x^2 - x + 1) &= (x^4 + 2x^2 - x + 2) - (x^3 - 2x^2 + 2x - 2)(x + 2) = \\ &= (x^4 + 2x^2 - x + 2) + ((x^5 - x^4 + x^3 - x^2 + x - 1) - (x^4 + 2x^2 - x + 2)(x - 1))(x + 2) = \\ &= (x^5 - x^4 + x^3 - x^2 + x - 1)(x + 2) - (x^4 + 2x^2 - x + 2)((x - 1)(x + 2) - 1) = \\ &= (x^5 - x^4 + x^3 - x^2 + x - 1)(x + 2) - (x^5 + x^3 + x^2 + 1 - (x^5 - x^4 + x^3 - x^2 + x - 1))(x^2 + x - 3) = \\ &= (x^5 - x^4 + x^3 - x^2 + x - 1)(x + 2 + x^2 + x - 3) - (x^5 + x^3 + x^2 + 1)(x^2 + x - 3) = \\ &= (x^5 - x^4 + x^3 - x^2 + x - 1)(x^2 + 2x - 1) - (x^5 + x^3 + x^2 + 1)(x^2 + x - 3). \end{aligned}$$

Следовательно, $P(x) = \frac{x^2}{4} + \frac{x}{2} - \frac{1}{4}$, $Q(x) = \frac{x^2}{4} + \frac{x}{4} - \frac{3}{4}$.